

**AFFIDAVIT OF SPECIAL AGENT JOHN H. McKEE IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, JOHN H. McKEE, state:

***INTRODUCTION AND AGENT BACKGROUND***

1. I have been a Special Agent (“SA”) with the United States Bureau of Alcohol, Tobacco, Firearms, and Explosives (“ATF”) since 2016 and am currently assigned to the ATF Boston Field Office’s Springfield Resident Office. In 2016, I completed an approximately twelve-week intensive Criminal Investigator Training Program and a fourteen-week ATF training course at the Federal Law Enforcement Training Center in Glynco, Georgia. During the course of my employment with the ATF, I have received specialized training regarding the activities of firearms trafficking and various aspects of firearms investigations. I have conducted numerous investigations of violations of federal firearms laws, including investigation of the unlawful possession of machineguns, so-called auto sears and conversion devices that convert semi-automatic weapons into machineguns, and silencers or mufflers in violation of the National Firearms Act (“NFA”) and the Gun Control Act (“GCA”).

2. In addition to my training, I have experience in investigating narcotics and firearm traffickers’ activities. I have been a member of the ATF’s Springfield Task Force (the “Task Force”) since 2016. Since joining the ATF, I have participated in approximately 50 narcotics investigations, both as a case agent and in subsidiary roles, regarding the distribution of controlled substances including cocaine, heroin, cocaine base, and other illegal substances. I have participated in more than 60 firearms investigations, both as case agent and in subsidiary roles, regarding the distribution and possession of firearms, including the use of firearms in connection

with drug distribution, as well as the illegal interstate and international trafficking of firearms. On a number of occasions, I have also debriefed informants, conducted surveillance, and participated in the preparation and execution of search warrants and arrest warrants. I have further served as the affiant and participated in the execution of numerous search warrants, and participated in court-authorized Title III wiretaps of cellular phones. I have received advanced training in how to conduct complex firearms trafficking investigations, have been certified as an Interstate Nexus Expert, and a Firearms Instructor.

3. Prior to working with the ATF, I was employed as an Investigative Specialist with the United States Federal Bureau of Investigation ("FBI") for approximately seven years. During that time, I was assigned to the Special Surveillance Group/Mobile Surveillance Teams of the San Francisco and Boston Field Divisions. In 2009, I completed an approximately ten-week intensive training program that consisted of training in foot and vehicular surveillance techniques, covert communications, tactical emergency vehicular operations, defensive tactics, counterterrorism investigations, and counterintelligence investigations. During my employment with the FBI, I participated in more than approximately 100 counterintelligence and terrorism investigations and received extensive training in those fields. I participated in many temporary duty assignments that involved traveling to various locations within the boundaries of the United States to assist in high-priority surveillance operations in support of a variety of case types investigated by the FBI.

4. I am currently investigating Daniel A. Augusto, Jr. ("Augusto") for violations of 18 U.S.C. § 922(a)(6) (False Statements Regarding Sales And Disposition Of Firearms); 922(o) (Unlawful Possession and Transfer of Machinegun), 924(a)(1)(A) (False Statements Regarding Records Of Federal Firearms Licensees), 922(a)(1)(A) (Unlawful Manufacturing and/or Dealing

Firearms Without Being Licensed), and 26 U.S.C. §§ 5861(d) and 5845(a)(6)-(7) (Unlawful Receipt And Possession Of Machineguns And Silencers) (the “Subject Offenses”).

5. I respectfully submit this affidavit in support of an application for warrants to search and seize the following, pursuant to Rule 41 of the Federal Rules of Criminal Procedure and/or 18 U.S.C. § 2703(a):

a. The residence of Augusto, located at 5 Robert Drive, Holyoke, MA, including any outbuildings, sheds, and storage locations (the “Subject Residence”), as further described in Attachment A-1.

b. The Facebook account identified by ID number 100000207447654 and name dan.augusto.9 and other data associated with this account (“the Subject Facebook Account”), as described in Attachment A-2;

c. The e-mail account identified as [pops1002@yahoo.com](mailto:pops1002@yahoo.com) and other data associated with this account (the “Subject Yahoo Account”) as described in Attachment A-3; and

d. The person of Augusto, as described in Attachment A-4  
(collectively, the “Subject Premises”).

6. As set forth below, because there is probable cause to believe that the Subject Residence, the Subject Facebook Account, and the Subject Yahoo Account contain evidence, fruits, and instrumentalities of the Subject Offenses, as described in Attachments B-1, B-2, B-3, and B-4.

7. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. I

am submitting this affidavit to show that there is probable cause for the requested search warrants and therefore the affidavit does not set forth all of my knowledge about this matter. Unless otherwise specified, all dates are approximate, all amounts are approximate, and all statements are in sum and substance.

***PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED***

Straw Firearms Purchases

8. “Before a federally licensed firearms dealer<sup>1</sup> may sell a gun, the would-be purchaser must provide certain personal information, show photo identification, and pass a background check. To ensure the accuracy of those submissions, a federal statute imposes criminal penalties on any person who, in connection with a firearm’s acquisition, makes false statements about ‘any fact material to the lawfulness of the sale.’” *Abramski v. United States*, 573 U.S. 169, 171 (2014) (quoting 18 U.S.C. § 922(a)(6)). In *Abramski*, the Supreme Court held that misrepresentations by a straw purchaser — “a person who buys a gun on someone else’s behalf while falsely claiming that it is for himself” — are punishable under Section 922(a)(6) “whether or not the true buyer could have purchased the gun without the straw.” *Id.* at 171-72.

9. “Relatedly, 18 U.S.C. § 924(a)(1)(A) . . . prohibits an individual from ‘knowingly mak[ing] any false statement or representation with respect to the information required by [Chapter 44 of Title 18] to be kept in the records of [an FFL].’ Although there is some overlap between these two provisions, § 922(a)(6) encompasses all materially false statements made regarding the legality of the firearm sale, whereas § 924(a)(1)(A) lacks a materiality requirement and applies only to statements made in records an FFL is required to maintain.” *United States v. Karani*, 984

---

<sup>1</sup> Federal firearms licensees, like gun shops, are commonly referred to as “FFLs.”

F.3d 163, 174 (1<sup>st</sup> Cir. 2021).

10. “The ‘twin goals’ of these provisions, within the broader statutory scheme, are ‘to keep guns out of the hands of criminals and others who should not have them, and to assist law enforcement authorities in investigating serious crimes.’” *Id.* (quoting *Abramski*, 573 U.S. at 180).

11. To complete the purchase of a firearm from an FFL, a purchaser must fill out ATF Form 4473, “a document that FFLs must use to gather the details that they are required by federal law to report about persons purchasing firearms.” *Id.* at 167 (citing 18 U.S.C. § 923(g); 27 C.F.R. § 478.124). This information includes the purchaser's name, address, date of birth, ethnicity, height, and weight. *Id.* The Form 4473 also assists FFLs in collecting the information needed for the criminal background checks required under federal law. *Id.* Form 4473 also contains a series of questions intended to assess whether an individual may lawfully purchase and possess a firearm. *Id.*

12. Title 18, United States Code, Section 922(a)(6) states:

(a) It shall be unlawful – [] for any person in connection with the acquisition or attempted acquisition of any firearm or ammunition from a licensed importer, licensed manufacturer, licensed dealer, or licensed collector, knowingly to make any false or fictitious oral or written statement or to furnish or exhibit any false, fictitious, or misrepresented identification, intended or likely to deceive such importer, manufacturer, dealer, or collector with respect to any fact material to the lawfulness of the sale or other disposition of such firearm or ammunition under the provisions of this chapter.

18 U.S.C. § 922(a)(6).

13. Title 18, United States Code, Section 924(a)(1)(A) states:

(a)(1) Except as otherwise provided in this subsection, subsection (b), (c), (f), or (p) of this section, or in section 929, whoever -- (A) knowingly makes any false statement or representation with respect to the information required by this chapter to be kept in the records

of a person licensed under this chapter . . . shall be [punished].

18 U.S.C. § 924(a)(1)(A).

Unlawful Manufacture And Dealing Of Firearms

14. Title 18, United States Code, Section 922(a)(1)(A) provides: “(a) It shall be unlawful -- (1) for any person-- (A) except a licensed importer, licensed manufacturer, or licensed dealer, to engage in the business of importing, manufacturing, or dealing in firearms, or in the course of such business to ship, transport, or receive any firearm in interstate or foreign commerce.” 18 U.S.C. § 922(a)(1)(A).<sup>2</sup>

15. Title 18, United States Code, Section 921(a)(3) defines a “firearm” as “any weapon (including a starter gun) which will or is designed to or may readily be converted to expel a projectile by the action of an explosive; the frame or receiver of any such weapon . . . .”

16. Title 18 United States Code, Section 921(a)(10) defines a “manufacturer” as “any person engaged in the business of manufacturing firearms or ammunition for the purposes of sale or distribution . . . .”

17. Title 18 United States Code, Section 921(a)(11) defines a “dealer” in pertinent part as “any person engaged in the business of selling firearms at wholesale or retail . . . .”

18. The term “engaged in the business” is further defined at 18 U.S.C. § 921(a)(21)(A) and (C), as follows:

- a. Section 921(a)(21)(A) defines a “manufacturer” as “a person who devotes time attention and labor to manufacturing as a regular course of trade or business

---

<sup>2</sup> To establish a willful violation of a statute, the Government must prove that the defendant acted with knowledge that his conduct was unlawful, not that he was aware of a particular licensing requirement. *Bryan v. United States*, 524 U.S. 184, 191-92 (1998).

with the principal objective of livelihood and profit through the sale or distribution of the firearms manufactured.” 18 U.S.C. § 921(a)(21)(A)

b. Section 921(a)(21)(C) defines a “dealer” as “a person who devotes time, attention and labor to dealing in firearms as a regular course of trade or business with the principal objective of livelihood and profit through the repetitive purchase and resale of firearms, but such term shall not include a person who makes occasional sales, exchanges, or purchases of firearms for the enhancement of a personal collection or for a hobby, or who sells all or part of his personal collection of firearms.” 18 U.S.C. § 921(a)(21)(C).

#### Illegal Possession of Machineguns and Silencers

19. Title 18, United States Code, Section 922(o) prohibits the transfer or possession of a machinegun as follows:

(1) Except as provided in paragraph (2), it shall be unlawful for any person to transfer or possess a machinegun.

(2) This subsection does not apply with respect to —

(A) a transfer to or by, or possession by or under the authority of, the United States or any department or agency thereof or a State, or a department, agency, or political subdivision thereof; or

(B) any lawful transfer or lawful possession of a machinegun that was lawfully possessed before the date this subsection takes effect.

18 U.S.C. § 922(o).

20. Title 18, United States Code, Section 921(a)(23) incorporates the definition of a machinegun in 26 U.S.C. § 5845(b): “The term ‘machinegun’ has the meaning given such term in section 5845(b) of the National Firearms Act (26 U.S.C. 5845(b)).”

21. Title 26, United States Code, Section 5845(b) defines “machinegun” as follows:

The term “machinegun” means any weapon which shoots, is designed to shoot, or can be readily restored to shoot, automatically more than one shot, without manual reloading, by a single function of the trigger. The term shall also include the frame or receiver of any such weapon, any part designed and intended solely and exclusively, or combination of parts designed and intended, for use in converting a weapon into a machinegun, and any combination of parts from which a machinegun can be assembled if such parts are in the possession or under the control of a person.

26 U.S.C. § 5845(b) (underlining added).

22. Title 26, United States Code, Section 5861(d) states: “It shall be unlawful for any person -- (d) to receive or possess a firearm which is not registered to him in the National Firearms Registration and Transfer Record.”

23. Title 26, United States Code, Section 5845(a)(6)-(7) provides: “For the purpose of this chapter-- (a) Firearm.--The term “firearm” means . . . (6) a machinegun; (7) any silencer (as defined in section 921 of title 18, United States Code).”

24. Title 18, United States Code, Section 921(a)(24) provides: “The terms ‘firearm silencer’ and ‘firearm muffler’ mean any device for silencing, muffling, or diminishing the report of a portable firearm, including any combination of parts, designed or redesigned, and intended for use in assembling or fabricating a firearm silencer or firearm muffler, and any part intended only for use in such assembly or fabrication.” 18 U.S.C. § 921(a)(24).

#### Auto Sear

25. The ATF has examined a part, commonly known as an “auto sear” and identified by various trade names, including “AR 15 auto sear,” “drop in auto sear,” and “auto sear II” (the “Auto Sear”). The ATF has found that the addition of the Auto Sear to certain AR15 type semi-automatic rifles, manufactured with M16 internal components already installed, will convert such



rifles to machineguns by enabling the firearm to shoot automatically more than one shot, without manual loading, by a single function of the trigger. Thus, the Auto Sear is “any part designed and intended solely and exclusively, or combination of parts designed and intended, for use in converting a weapon into a machinegun” and, consequently, constitutes a machinegun as defined by 26 U.S.C. § 5845(b). *See* 27 CFR 179.11.

26. I incorporate herein the Affidavit of Special Agent Mark McNeal in support of a Criminal Complaint against Timothy John Watson (“Watson”), sworn to on October 30, 2020, in *United States v. Timothy John Watson*, Criminal Docket No. 20-CR-00042-GMG-RWT (N.D.W.Va.) (D.1) (the “McNeal Affidavit”).<sup>3</sup> A copy of the McNeal Affidavit is attached hereto as Exhibit 1.

27. As set forth in greater detail in the McNeal Affidavit, Watson operated an online retail business, “portablewallhanger.com,” that purported to sell innocuous 3D-printed, two-piece hooks; however, when disassembled, one of the pieces functions as an illegal Auto Sear that converts a semi-automatic AR-15 rifle into a fully automatic machinegun. *Id.* at ¶ 9. Watson used e-mail, Instagram, and Paypal accounts, as well as a website named portablewallhanger.com, to conduct his business, including to communicate with customers and conduct transactions. *Id.* at ¶¶ 14-18 and *et seq.* On or about October 15, 2020, a paid confidential human source handled by

---

<sup>3</sup> In the *Watson* case, on November 17, 2020, Watson was indicted with one violation each of 18 U.S.C. § 371 (Conspiracy), 26 U.S.C. § 5861(a) (Unlawfully Engaging in the Business of Manufacturing Machineguns), 18 U.S.C. § 922(o) (Illegal Possession and Transfer of Machineguns), and 26 U.S.C. § 5861(d) (Possession of Unregistered Firearms Silencer). D.23. On March 16, 2021, pursuant to a written plea agreement, Watson pleaded guilty to Count Four, and the Government dismissed the first three counts but took the position at sentencing that Watson’s conduct involved the manufacture and transfer of hundreds of machinegun conversion devices for AR-15 style rifles – *i.e.*, the Auto Sear. D.50-53. On October 13, 2021, Watson was sentenced to 60 months of incarceration. D.67.

the FBI placed an online order for various items through Watson's website. On or about October 26, 2020, the FBI obtained the ordered package and transferred custody of it to the ATF, which determined that it contained six self-described "hooks" that operated as Auto Sear. *Id.* at ¶¶ 67-74.

#### Glock Conversion Devices

28. Based upon my training and experience, I am aware of conversion devices that have been designed and created for the sole purpose of converting semiautomatic Glock pistols into fully automatic machineguns. These devices vary by design and appearance but all, when properly installed on a semi-automatic Glock pistol, will allow the firearm to expel more than one projectile by a single pull of the trigger at approximately 1,200 rounds per minute. Installation of these conversion devices is fast and simple, requires no technical expertise, and is completed by removing the polymer slide cover plate on a Glock semi-automatic pistol and replacing it with a conversion device. I also know that these devices are referred to by different names, including but not limited to switches, auto sears, convertors, conversion switches, selector switches, conversion devices, and Fire Selector Systems for Glock ("FSSGs").

29. I know that ATF considers Glock conversion devices as post-May 19, 1986, machineguns. Therefore, apart from official military and law enforcement use, Glock conversion devices may only be lawfully possessed by properly licensed FFLs who have paid the appropriate Special Occupational Tax ("SOT") required of individuals manufacturing, importing, or dealing in NFA weapons, including machineguns.

#### Augusto's Purchase Of An Auto Sear From Portablewallhanger.com

30. According to PayPal records for portablewallhanger.com, on or about February 9,

2020, the company sold and shipped a family size portable wall hanger for \$36.48. The listed shipping address for the transaction was “Dan Augusto, 5 Robert Drive, Holyoke, MA 01040” – which I believe refers to Augusto and the Subject Residence. The listed e-mail for the transaction was [pops1002@yahoo.com](mailto:pops1002@yahoo.com). The listed purchase name was “Tombstone Productions.”

31. According to the results of a public search of the Dun & Bradstreet online business directory for Tombstone Productions dated January 6, 2021, Tombstone Productions is located at the 5 Robert Drive, Holyoke, MA (*i.e.*, the Subject Residence), its contact person is “Dan Augusto” (*i.e.*, Augusto), and its contact phone is (413) 534-5238.<sup>4</sup>

32. According to PayPal records of registration information for the users “Daniel Augusto,” “Dan Augusto,” and “Daniel Augusto, Sr.” the primary listed address is 5 Robert Drive, Holyoke, MA (*i.e.*, the Subject Residence and the address associated with the wall hanger purchase);<sup>5</sup> the listed e-mail accounts include [pops1002@yahoo.com](mailto:pops1002@yahoo.com) (the e-mail account associated with the wall hanger purchase), [daugusto@comcast.net](mailto:daugusto@comcast.net), [daugusto@rcn.com](mailto:daugusto@rcn.com), and [daugusto@javanet.com](mailto:daugusto@javanet.com); the listed telephone numbers include (413) 534-5238, (413) 537-3510, and (413) 210-4223; and the listed business is Tombstone Productions.

#### Augusto’s PayPal Purchases of Fuel Filters and/or Solvent Traps

33. According to PayPal records, Augusto’s PayPal account engaged in the following transactions at Alipay Singapore E-Commerce Private Limited:

- a. December 20, 2020: \$73.55 purchase of “8.6 inch OD 1.7 Aluminum Car

---

<sup>4</sup> <https://www.dandb.com/businessdirectory/tombstoneproductions-holyoke-ma-10709877.html>.

<sup>5</sup> Other listed addresses are: (1) 52 Taylor Street, Holyoke, MA, which was added on May 24, 2013 and listed as ‘home or work’; and (2) 179 Dagget Drive, West Springfield, MA (use as gift).

Fuel Filter Solvent Traps cups adapter 5/8x24 & 1/2x28 For NAPA 4003 WIX 24003.”

b. December 24, 2020: \$99.89 purchase of “Aluminum sprial [sic] 1/2x28 Fuel Filter For NaPa [sic] 4003 Car 8.8 inch solvent traps adapter US.”

34. According to PayPal records for each of these transactions, the listed “From E-Mail Address” was the Subject Yahoo Account and the shipping address was the Subject Residence.

35. Based upon my training and experience, I know that individuals seeking to procure illegal firearms will frequently purchase fuel filters and/or solvent traps to use as silencers or mufflers on their firearms, or to modify them for use on firearms as silencers/suppressors, and that such users will frequently use the Internet to discuss such use. *See, e.g.*, [Fuel Filter Suppressor? Read Before You Make a Suppressor – KMwhisper](#) (stating, *inter alia*, “[t]he fuel filter suppressor is a type of ‘do it yourself’ suppressor. Most people may think that a fuel filter’s only potential is to remove contaminants from engine oil. However, oil filters can be used as an alternate gun suppressor.”); [Are solvent traps legal? – KMwhisper](#) (describing how a solvent trap suppressor works and stating, *inter alia*, “[a] suppressor is a controlled item also an NFA (National Firearms Act) item. Federal law requires that anyone who [builds a solvent trap suppressor] still register the device, and submit it to a background check before construction.”); [Gear Review: \\$39 'Fule Filter' Form 1 Silencer Build \[VIDEO\] - The Truth About Guns](#) (stating “[t]here a handful of products that are readily converted into a firearm silencer, including solvent traps [], oil filter adapters, [and] ‘fule filters’ [sic].”)

36. Based upon my training an experience, I know that legitimate solvent traps are devices attached to the muzzle of a firearm barrel designed to catch or “trap” dirty cleaning solvent

pushed through the barrel from the chamber end and out through the muzzle. Solvent traps are intended to prevent solvent from dripping, spraying, or spattering when pushed out the muzzle end of a firearm barrel. The front endcap of a solvent trap must be solid and have no hole that will allow a projectile to pass-through (including “pilot” holes that can be widened to allow a projectile to pass-through or marks indicating the location to drill such a hole). Devices that have a hole in or indexing mark for a hole in the front endcap are classified as a “firearm silencer” under the NFA.

37. The thread diameters “1/2x28” and “5/8x24” listed in the product descriptions of the “fuel filter” / “solvent trap” items in the Augusto PayPal records for the December 20, 2020 and December 24, 2020, indicate the items come with adapters in those dimensions. Based upon my training and experience, these described adapters match the diameters of the threads that are commonly found on the end of barrels for most 5.56 / .223 caliber, .308 caliber, 9mm caliber, and .22LR caliber firearms.

38. Based upon my training, experience, and knowledge of the case, I believe that Augusto conducted the Paypal transactions for the fuel filters and/or solvent traps to use as illegal silencers or mufflers on firearms.

#### Augusto’s Admissions Regarding Illegal Firearms Purchases And Possession

39. On October 30, 2020, Holyoke Police Department (“HPD”) Officer Andrew Urbanski (“Officer Urbanski”) wrote a letter to HPD Lieutenant James Albert that stated in pertinent part:

I have known D. Augusto for at least the last 15 or so years from my involvement working at McCray’s Farm and assisting with the Haunted Hayride in which D. Augusto runs and operated. [] During my time working for him, he would always talk about different guns

he has. He mentioned on several accounts that he has the capabilities to make his Glock pistols go fully automatic and had large capacity magazines for them. He also talked about high capacity rifles he has like the UZI and UMP he has and mentioned how he orders drop in trigger kits for his assault rifles to make them fully automatic. He also spoke about having “cans” which was a reference to a silencer. I am not sure if they are real ones or just a solvent trap style but nonetheless, he made it abundantly clear he had them.

I do not believe he belongs to any firing range but rather just shoots out on McCray’s property. Several years ago, he was shooting the insulators on the high tension wires and when confronted about it, denied shooting them and instead blamed the damage to them on another individual and myself.

Regarding purchasing these weapons, I personally witnessed him at gun shows looking at guns, then handing his father a wad of cash and had his father purchase the guns. I confronted him about this and told him that this is a straw purchase. He denied everything saying the gun was for his father and they were not for him but a few weeks later he would be posting on “Facebook” that he purchased a new gun and it would be the same one from the gun show. I know he recently has connections to a gun shop in Turners Falls as well as another gun shop in Agawam where his son Tyler works.

40. Based upon my training and experience, I know that a common term for a firearm silencer is a “can.” As set forth above, I also know that a “solvent trap style” suppressor/silencer is a specific reference to the “solvent trap/fuel filter” kits that are able to be purchased over the internet via several overseas retailers. These “solvent trap/fuel filter” kits can be modified by individuals for use as firearm suppressor/silencers.

41. On October 6, 2021, Federal Bureau of Investigation Special Agent Ryan McGonigle (“Special Agent McGonigle”) interviewed Officer Urbanski, who stated:

a. Augusto was looking to purchase illegal or legally questionable guns or gun paraphernalia.

b. When Officer Urbanski was serving in the United States Marine Corps (“USMC”), Augusto asked him if he could get or steal guns or night vision equipment from the USMC.

c. When Officer Urbanski worked at the firearms manufacturer Smith & Wesson (“S&W”), Augusto talked with him about the S&W guns that could be altered to become fully automatic.

d. On approximately thirty to forty occasions, Augusto told him that he made his Glock handgun fully automatic. Augusto has also told him that he purchased items like a drop-in auto sear to make his weapons fully automatic.

42. On October 7, 2021, Federal Bureau of Investigation Special Agent Ryan McGonigle interviewed a former associate and co-worker of Augusto, who stated:

a. He knows Augusto because he used to work at McCray’s Farm, where Augusto ran a Haunted Halloween exhibit. They connected over their shared interest in firearms.

b. Augusto frequently talked about acquiring questionably legal weapons or buying items to convert legal weapons into illegal weapons.

c. Specifically, Augusto stated that he had purchased a Glock trigger switch that converts a Glock into an automatic weapon, and drop-in auto sear that makes a semi-automatic assault rifle fire in an automatic manner. Augusto told him that the drop-in auto sear was a legal part but could not be placed into the gun.<sup>6</sup>

---

<sup>6</sup> The former co-worker and associate also stated that he has distanced himself from Augusto and that it has been years since he spoke with Augusto about weapons.

d. He recalled seeing Augusto purchase a machinegun at a gun show, but assumed that the machinegun was a pre-ban weapon because it was being sold at the gun show.

Firearms Related Financial Transactions Of Augusto

43. According to HPD Incident Report No. 19-3481-OF, on July 25, 2019, HPD officers responded to the Subject Residence following a report of a sudden death at the house. The HPD officers learned that Daniel A. Augusto, Sr. (*i.e.*, Augusto's father) had died. While at the home, the officers met with Augusto; Augusto's live-in girlfriend, Brigetann Reilly ("Brigetann"); and their respective adult sons, Tyler Augusto ("Tyler") and John Reilly ("John").

44. I have conducted a preliminary review of a PeoplesBank account (x-1044) in the joint names of Augusto's father and Augusto (the "Augusto PeoplesBank Account"). The listed address for the Augusto PeoplesBank Account is 5 Robert Drive, Holyoke, MA 01040 - *i.e.*, the Subject Residence. According to my review, the Augusto Joint Account engaged in numerous, large, apparently firearms-related both before, and after, Augusto's father died on July 25, 2019. Between December 10, 2018 and November 8, 2021, the Augusto PeoplesBank Account engaged in approximately 100 transactions totaling approximately \$28,015 with vendors preliminarily identified as vendors of firearms and/or firearms parts/accessories.

45. Notably, the Augusto PeoplesBank Account engaged in numerous firearms-related transactions after Augusto's father died. For example, according to the account records, on March 27 and 30, 2020 (*i.e.*, less than two months after the wall hanger purchase), the account engaged in the following transactions:

a. On March 27, 2020: \$164.90 point of sale withdrawal at Black Rifle Depot.



According to its website, Black Rifle Depot “offer[s] a large variety of American made AR 15 Parts. Such as AR 15 Complete Uppers, AR 15 Barrels, AR 15 Bolt Carriers, AR 15 Handguards, AR 15 Lower Build Kits, and AR 15 Rifle Build Kits to customize your AR 15 Rifle.”<sup>7</sup>

b. On March 30, 2020: \$64.98 point of sale withdrawal at 5D Tactical. According to its website, “5D Tactical supplies essential equipment for building your own AR-15, AR-9 or AR-308/AR-10 firearms.”<sup>8</sup>

c. On October 13, 2020: \$478.13 point of sale withdrawal at The Gun Rack, an FFL located in Turners Falls, MA. A review of the MA firearms transaction record for Tyler Austin Augusto (*i.e.*, Augusto’s son Tyler) shows that on October 14, 2020, Tyler purchased a Sig Sauer 9mm caliber firearm bearing serial number NRA023994 from The Gun Rack.

d. On November 27, 2020: \$573.75 point of sale withdrawal at The Gun Rack. A review of the MA firearms transaction record for Tyler shows that on November 27, 2020, Tyler purchased a Colt .223 caliber firearm bearing serial number SP41339 and a Taurus 9mm caliber firearm bearing serial number GP55413 from The Gun Rack.

e. On October 28, 2021: \$1,593.74 point of sale withdrawal at The Gun Rack. A review of the MA firearms transaction record for Tyler shows that on October 28, 2021, Tyler purchased a Sig Sauer 5.56mm caliber firearm bearing serial

---

<sup>7</sup> <https://blackrifledepot.com>.

<sup>8</sup> <https://www.5dtactical.com>.

number NRA023994 from The Gun Rack.

46. Based upon my training, experience, and knowledge of the case, I believe that these transactions may be straw purchases by Tyler for his father, Augusto.

Use Of “80% Receivers” To Manufacture Firearms

47. In firearms terminology, the “receiver” is the part of a firearm that houses the operating parts. There are many types and styles of firearm receivers. The term “80% receiver” is industry vernacular that refers to an unfinished firearm that has not yet reached the point in the manufacturing process where it should be classified as a “firearm” as defined by 18 U.S.C. § 922(a)(3). The unfinished receivers are usually fabricated to a point where minimal work needs to be completed by the purchaser in order to convert it into a “firearm.”

48. Since “80% receivers” do not meet definition of a firearm, they are not subject to the same requirements to purchase, transfer, or possess. “80% receivers” can be purchased by anyone, including prohibited persons, such as persons previously convicted of a crime punishable by more than one year in prison, and are often purchased through the Internet with no record keeping requirements.

49. There are several methods to “manufacture” the unfinished receiver into a firearm. Some of these methods involve milling out or drilling the unfinished receiver.

50. This can be accomplished by using different types of tools or machines such as a drill press, a milling machine, or a computer numerical control (“CNC”) milling machine. CNC milling is a machining process that uses computerized controls and rotary cutting tools to progressively remove material from the working item, resulting in a custom-designed part or product.

51. The process of drilling out or milling out the unfinished receiver generally creates metal shavings on or around the used equipment. Often, the unfinished receiver will come with a template to guide where milling or drilling must occur in order to complete the firearm.

52. Once the receiver has been completed, it is usually affixed with other firearms parts and accessories that constitute a firearm under federal law. There are numerous parts and accessories that can be added to the receiver, such as barrels, stocks and triggers. These individual parts and accessories can also be purchased by any individual, including prohibited persons.

#### Augusto's Purchases from Defense Distributed

53. According to its website, "Defense Distributed is the first private defense contractor in service of the general public. Since 2012's Wiki Weapon project, DD has defined the state of the art in small scale, digital, personal gunsmithing technology."<sup>9</sup> Defense Distributed's website advertises various products, including the "Ghost Gunner 3" or "GG3," which the company states "allows you to manufacture firearms with confidence and ease, in the privacy of your own home. GG3 removes material 5 times faster than GG2 and the new unibody construction provides greater rigidity, drastically improving finished part quality."

54. The "GG3" is a microwave-sized CNC milling machine that can be used to complete "80% receivers" and/or create firearm frames/receivers from production material. These machines are operated with this assistance of a computer that needs to be loaded with the appropriate software to operate the CNC milling machine. Defense Distributed provides the software to the users of the "GG3" so that they can finish the frame or receiver. The website also states that the "GG3 ships with code to complete 80% AR-15, AR-308, M1911, Polymer 80 and

---


<sup>9</sup> <https://defdist.org>

AK-47 lowers and frames” and that the GG3 includes a “DD USB with all our latest software” which I understand to mean that Defense Distributed provides its customers with software that enables them to use the GG3 to manufacture firearms.


55. According to its website, Defense Distributed sells the GG3 for \$2,500, including a \$500 non-refundable deposit and excluding a shipping cost of \$225.

56. In addition, Defense Distributed sells a variety of starter kits, including for the AR-15, AK-47, and AR-308 semi-automatic rifles, and the M1911 pistol, as well as a selection of 80% lowers and frames for these firearms, as set forth below:


### Starter Kits




Polymer80 Starter Kit  
\$241.98  
[Add to cart](#)




AR-15 Starter Kit  
\$104.48  
[Add to cart](#)




AK-47 Starter Kit  
\$266.00  
[Read more](#)



Zero Percent Starter Kit  
\$295.00  
[Add to cart](#)




AR-308 Starter Kit  
\$116.58  
[Add to cart](#)




M1911 Starter Kit  
\$297.00  
[Add to cart](#)


### 80% Lowers & Frames




AR-15 80% Lower Receiver - Forged  
\$49.99  
[Read more](#)




AK-47 80% Lower Receiver  
\$114.99  
[Add to cart](#)




AR-15 80% Lower Receiver  
\$115.00  
[Add to cart](#)




AR-308 80% Lower Receiver  
\$119.00  
[Add to cart](#)



M1911 80% Frame: .45ACP  
\$165.00  
[Read more](#)



M1911 80% Frame: 9mm/10mm/.38 Super/.40 S&W  
\$165.00  
[Read more](#)



Polymer80 80% Frame  
\$176.00  
[Read more](#)

**Ghost Gunner Newsletter:**  
News, Product Releases, Resources:

[SUBSCRIBE](#)
[CLOSE](#)

[Support](#)

57. As set forth above, the Defense Distributed website also allows interested individuals to obtain a subscription to the “Ghost Gunner Newsletter” by entering their e-mail address, and it features a “Support” button which, if clicked, prompts the user to enter their e-mail address, questions, and attached digital files for online support.

58. According to my review of the Augusto PeoplesBank Account, the account conducted three check/wire payments to Defense Distributed:

- a. November 12, 2020: \$1,790.90 with memo line “Order 28428.”
- b. August 10, 2021: \$213.90 with memo line “Order 35850.”
- c. November 2, 2021: \$224.75 with memo line “Order 37686.”

59. All checks bear the name “Dan Augusto,” which I believe refers to Augusto; and the address of the Subject Residence. The first two checks also bear the telephone number 413-537-3510, which I believe is used by Augusto; and the third check bears the e-mail address [DAUGUSTO@COMCAST.NET](mailto:DAUGUSTO@COMCAST.NET), which as set forth below is one of the registered e-mail addresses for the Subject Facebook Account.

60. Based upon my training, experience, and knowledge of the case, I believe that Augusto has conducted these transactions with Defense Distributed, as well as other financial transactions with the Augusto PeoplesBank Account, so that he can engage in the personal manufacture of firearms.

Federal Licensing System and National Firearms Registry and Transfer Record Query

61. On February 1, 2022, I conducted an online query of the Federal Licensing System (FLS) to identify any FFL holders affiliated with the Subject Residence. The results yielded one license: a Type 03 Curio and Relic (“C&R”) Federal License Number “6-04-013-03-3C-14394”

in the name of “Tyler Austin Augusto” (*i.e.*, Augusto’s son) with the address of “5 Robert Drive, Holyoke, MA” (*i.e.*, the Subject Residence) and the listed business activity of “Collector.”<sup>10</sup> The query did not identify any licenses for Augusto, and no licenses for any residents of the Subject Residence to manufacture firearms.

62. On February 1, 2022, I also requested a query be conducted of the National Firearm Registration and Transfer Record (“NFRTR”) to determine if any NFA weapons have ever been registered/transferred by any of the known residents of the Subject Residence. On February 2, 2022, I received results that showed that no residents of the Subject Residence have ever registered/transferred an NFA weapon.

***THE SUBJECT RESIDENCE CONTAINS EVIDENCE, FRUITS, AND  
INSTRUMENTALITIES***

63. I also have probable cause to believe that the Subject Residence contains fruits, evidence, and instrumentalities of violations of the Subject Offenses, as described in Attachment B.

The Subject Residence

64. Based upon the information above, I believe that the primary residents of the Subject Residence are Augusto; his son Tyler; his live-in girlfriend Reilly; and her son John.

---

<sup>10</sup> A Type 03 FFL issued under 18 U.S.C. Chapter 44 is not a license to carry, use, or possess a firearm. It confers no right or privilege to conduct an activity contrary to State or other law. It entitles a person to acquire firearms, classified as curios or relics, in interstate or foreign commerce. One may dispose of curios and relics to any person, not otherwise prohibited by the Gun Control Act of 1968, residing within one’s State, and to any other Federal firearms licensee in any State. A Type 03 FFL license pertains exclusively to firearms classified as curios and relics, and its purpose is to facilitate a personal collection. One may not engage in the business of buying and selling any type of firearm with a Type 03 FFL. Applicants intending to engage in the firearms business should apply for a license other than a Type 03, Collector of Curios and Relics, license.

65. On January 2, 2022, I conducted physical surveillance of the Subject Residence. I observed a vehicle in the driveway with MA license plate number 4KC239. According to the MA RMV, this vehicle is registered to Dan Augusto, Jr. (*i.e.*, Augusto) at the Subject Residence.

66. On January 11, 2022, I requested ATF Task Force Officer (“TFO Dave Seidel”) to conduct physical surveillance of the Subject Residence. TFO Seidel observed the following vehicles in the driveway of the Subject Residence:

- a. The vehicle with MA license plate 4KC239.
- b. A vehicle with MA license plate number 4MTL29. According to the MA RMV, this vehicle is registered to Tyler Austin Augusto (*i.e.*, Augusto’s son Tyler) at the Subject Residence.
- c. A vehicle with MA license plate number 315HL1. According to the MA RMV, this vehicle is registered to Brigetann Reilly (*i.e.*, Augusto’s live-in girlfriend) at the Subject Residence.

67. On January 18, 2022, I queried the MA Criminal Justice Information System (“CJIS”) for any individuals with a Massachusetts license to carry firearms (“LTC”) at the Subject Residence. According to records kept by the Commonwealth of Massachusetts, the following individuals possess active MA LTCs at the Subject Residence:

- a. Dan Augusto Sr. (Augusto’s now deceased father): MA LTC 12780813A;
- b. Tyler Austin Augusto (Augusto’s son): MA Types C & F LTCs 12985100A and 31085159C and;
- c. Brigetann Reilly (Augusto’s live-in girlfriend): MA Type C LTC 13158148A.

68. On January 20, 2022, I conducted physical surveillance of the Subject Residence. I again observed 4KC239 parked in the driveway of the Subject Residence.

Massachusetts Firearms Ownership Records For Residents Of The Subject Residence

69. The Massachusetts Department of Criminal Justice Information Services (“DCJIS”) manages and administers the Commonwealth’s law enforcement information and criminal records systems, including records of firearms ownership maintained by the Firearms Records Bureau (“FRB”). The FRB is the Commonwealth’s repository for firearms license and transaction data.

70. According to the FRB’s website,<sup>11</sup> Massachusetts residents must obtain licenses to carry (“LTCs”) certain firearms (LTC) and firearms identification (“FID”) cards for firearms generally. Both LTCs and FID cards are issued to residents by the police department where the individual either resides or has a place of business. To possess a non-large capacity rifle and shotgun in one’s home, an individual needs an FID card. To possess a handguns or other large capacity firearm, an individual needs an LTC.

71. According to the FRB’s website,<sup>12</sup> Massachusetts law permits a properly licensed resident who is not a dealer to sell up to four guns in any one calendar year through a private transfer of ownership, and certain exemptions apply in the event of an inheritance. Massachusetts law requires all residents to report any private sale or transfer of a firearm via the Massachusetts Gun Transaction Portal either prior to, or at the time of the sale/transfer. Massachusetts law also requires all residents who purchase or obtain a firearm by any means other than by a personal

---

<sup>11</sup> <https://www.mass.gov/info-details/firearms-license-frequently-asked-questions>.

<sup>12</sup> *Id.*



sale/transfer or through a Massachusetts firearms dealer to register the firearm within 7 days using the Massachusetts Gun Transaction Portal. Inherited firearms may also be registered or transferred using the Portal.

72. On February 16, 2022, I conducted queries Firearms Ownership through the CJIS database for all of the individuals whom I believe currently reside at the Subject Premises (Augusto; his son, Tyler; his live-in girlfriend Brigetann; her son, John), as well as Augusto's deceased father, Augusto, Sr. The results of these queries, which identify the firearms by serial number, are attached as Exhibit 2 to each of Attachments B-1 through B-4. These results simply indicate that at some point in time, the acquisition of these firearms by these individuals was registered with the FRB. These results do not necessarily indicate that these individuals currently possess these firearms or that they are necessarily in the Subject Residence, since some or all may have been transferred by these people to other individuals without recorded the transfers in the FRB database. I have summarized the results below:

<b>Name</b>	<b>Number of Firearms</b>
Augusto	Zero
Augusto, Sr.	35
Tyler	90
Brigetann	27
John	Zero

#### The Use Of Residences To Conduct And Facilitate Firearms Offenses

73. Based on my training and experience, I know that individuals who own or possess

firearms generally keep them on their person, in their residence, on their property, or in their vehicles to afford ease of access and to provide security. Further, individuals who manufacture firearms without a license, often use their residence as a workspace or to store parts and tools associated with their activities. Firearms are relatively expensive and do not easily wear out and therefore individuals maintain them over a long period of time. Further, I know that most people store their firearms related materials (ammunition, cleaning kits, manuals, etc.) in their homes, on their property or in their vehicles. These components are likely to be located in proximity to or in the firearms with which they are intended to be used.

74. Based on my training and experience, I know that people research how to manufacture firearms, and manufacture “80% receivers” into actual “firearms” by searching the internet and/or reading firearms books/manuals. I also know that people order parts/components to do so via the internet and store these materials on their computers at their homes. As set forth above, Augusto has purchased numerous firearms-related items over the Internet.

75. Based on my training and experience I know that individuals who manufacture firearms use machines and tools to do so. The tools can include a variety of machines, which could include, milling machines, drill presses, or other hand tools. I know that individuals who manufacture firearms from “80%” receivers, use the aforementioned tools and machines to finish to complete the manufacturing process and make a “firearm” receiver (frame). This receiver is then assembled with other firearms parts components in order to make a functioning firearm. These other firearms parts and components can be purchased locally or through the Internet and are generally stored in the individual’s residence, or in close proximity to or affixed to the firearm receiver.

76. Based on my training and experience I know that individuals who purchase firearms and firearms components, both from stores and online entities, receive physical and electronic records and receipts relating to their purchases. These records are usually included with purchased firearms and firearms components during shipment, and these individuals typically keep these records at their residences.

77. I also know, based upon my training and experience, that with the proper knowledge, computer software, and machining equipment, individuals have the ability to manufacture both semi-automatic firearms and fully automatic machineguns from scratch. These firearms can be manufactured with the use of lathes or CNC, which are digitally automated machining centers capable of cutting and fabricating solid materials including firearms parts. With this type of equipment, a subject can manufacture firearms that perform as well as those created by FFL manufacturers, and can place on the firearms any type of markings, symbols, or serial numbers the subject desires.

78. Based upon my experience in conducting criminal investigations of violations of federal firearm and ammunition laws, I know that illegal firearm manufacturing organizations have developed a number of methods to insulate their illegal activities from law enforcement detection. These methods are common to major firearm and ammunition manufacturing organizations to varying degrees of sophistication.

79. I know that illegal firearm manufacturers/possessors often use techniques to prevent the detection of firearms that are shipped unlawfully through mail and common carriers by means of falsifying invoices, bills of sale, shipping papers, and customs forms by listing the firearms as other items, including but not limited to firearms parts and pieces (rather than complete

firearms) and components used in the automotive, industrial, and machinery industries. In addition, illegal firearm manufacturers/possessors often conceal firearms inside of other objects to avoid detection by law enforcement officials.

80. I know that another common technique of illegal firearm manufacturers/possessors is the use of latex and vinyl gloves by individuals handling firearms and ammunition while processing packages for shipment. This is done in order to prevent fingerprints from being left on items that could later be used as evidence against such individuals.

81. I know, based upon experience, that one key indicator of illegal firearm manufacturers/possessors is the use of complex methods for ordering, paying for, and transferring the firearms, firearm components, and/or ammunition. I know that illegal firearm and ammunition traffickers use payment methods that are often difficult to trace, which include utilizing U.S. currency, money orders, wire-transfers, PayPal accounts, and/or pre-paid credit cards held by different subjects. Illegal firearm and ammunition traffickers use these methods as a means of compartmentalization in order to minimize the ability for law enforcement officials to identify the original source of funds.

82. I know that illegal firearm manufacturers/possessors often use cellular telephones that are held in the names of other living or fictitious persons, and change numbers frequently in order to limit law enforcement officials' ability to identify and track suspects' call histories. In addition, I know that illegal firearm manufacturers/possessors often use computers and electronic storage devices to acquire, pay for, sell, transfer, and keep records of firearm purchases and sales. Firearm manufacturers/possessors also use code words for quantities and types of firearms and ammunition that are being purchased, sold, and/or transferred in effort to avoid detection by law

enforcement officials.

83. Based on my training and experience, and participation in illegal firearms manufacturing /possession investigations, I know:

- a. That illegal firearm manufacturers/possessors normally keep firearms in their homes, on their person, on their property, or in their vehicles. Firearms manufacturers/possessors consider these items as highly sought after commodities and as such assign significant value to them. They keep these commodities in the homes, on their person, on their property, or in their vehicles in an effort to provide security for their firearms and to keep their activities clandestine as sometimes their possession, brandishing, and use of these items is illegal and they are constantly aware of law enforcement's efforts to discover their activity.
- b. That illegal firearm manufacturers/possessors commonly maintain names and contact information in books, ledgers, telephones, computers, electronic tablets such as iPads, other digital devices, and digital storage media, which reflect the names, addresses, telephone numbers, and email addresses of their firearms sales customers.
- c. That illegal firearm manufacturers/possessors frequently take or cause to be taken photographs of themselves, their associates, their property, and their firearms and illicit proceeds. These illegal firearm manufacturers/possessors usually maintain these photographs in their residences, electronic devices used by them, or in properties owned or rented by them.
- d. That illegal firearm manufacturers/possessors who have amassed proceeds

from their firearms manufacturers/possessors will often attempt to legitimize these profits. In this process illegal firearm manufacturers/possessors often use, among other things, banks and their attendant services, securities, cashier's checks, money drafts, wire transfers, real estate, shell corporations, business funds, and vehicles. Records evidencing such services, items, and transactions are maintained where the illegal firearm manufacturers/possessors have ready access to them, including their residences, electronic devices used by them, or in properties owned or rented by them. These items can remain at the illegal firearm manufacturers/possessors property for a long period of time.

#### Seizure of Computer Equipment and Data

84. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e mail, instant messages, and updates to online social networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

85. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B in computer hardware, computer software, computer-related documentation, and storage media.

86. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the

internet. This is true because:

87. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

88. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.

89. Wholly apart from user generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

90. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

91. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in

computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media (“computer equipment”) be seized and subsequently processed by a qualified computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

92. The volume of evidence storage media such as hard disks, flash drives, CD-ROMs, and DVD-ROMs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on site.

93. Technical requirements – analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, password protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely



vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

94. Consequently, law enforcement agents may either copy the data at the Subject Residence to be searched or seize the computer equipment for subsequent processing elsewhere.

95. The Subject Residence may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner’s knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the Subject Residence during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how their contents or ownership appear or are described by others at the scene of the search.

96. Therefore, there is probable cause to believe that the Subject Residence will contain: (a) firearms manufacturing proceeds being stored, deposited, concealed, used in monetary and financial transactions and laundered; (b) the firearms and related items purchased online by Augusto and ultimately delivered to the Subject Residence, and related documentation and/or software; and (c) other evidentiary items associated with ordering and purchase of items from online websites, such as digital receipts, shipping confirmations, delivery confirmations, etc.

#### The Subject Facebook Account

97. The Subject Facebook Account and relevant data is maintained by Facebook, Inc., which, Government databases indicate, accepts service of process at 1601 Willow Road, Menlo

Park, CA 94025 and via its law enforcement portal at [www.facebook.com/records](http://www.facebook.com/records).

98. Facebook is an online social networking service accessible at the website [www.facebook.com](http://www.facebook.com) or via an application (“app”) that can be installed on computer equipment, including a tablet or a cell phone. Facebook allows users to create profiles and share personal and biographical information; share content and media, including by uploading photographs and videos and sending links to other content; and communicate with other users in a variety of ways, from public discussions to private messaging.

99. When a user creates a Facebook account, they provide Facebook with information to begin building their online Facebook profile, including uploading at least one photo and selecting a Vanity Name and email address that will be associated with the account. The user may choose to provide other information as well for the “About Me” section of the page, including basic information such as where the user lives, works, and attends/attended school. This information is then displayed on the user’s page. The user may also provide Facebook with other contact information, such as phone numbers and email addresses. In addition, Facebook captures certain basic information about the new account, including the registration date and the IP address used to create the account. Further, Facebook assigns a unique numerical identifier to the account.

100. Facebook users can continually build their online profile, and in my training and experience it is common for users to add and edit biographical information – for instance by updating on a new job or changing a “relationship status” to reflect changes in their life. Facebook actively prompts users to provide or confirm information, for instance by asking the user to confirm that they live in a particular city if other information in the profile or the majority of connections suggests that they might live in that city. As a result, Facebook users typically provide a significant

amount of biographical information.

101. Facebook also encourages users to form connections with other users on the site, most fundamentally by allowing users to connect as “Friends.” A Facebook user creates a “Friend” connection by inviting another Facebook user to confirm that they are “Friends.” When the request is accepted, the connection is created. Facebook also prompts users to connect with other users when they share common connections.

102. Facebook offers users a variety of privacy settings. The Vanity Name and the Profile Picture and Cover Photo are publicly visible to anyone that visits the page, and are generally searchable unless a user has selected not to be searchable. Facebook users can keep their entire profile open publicly as well, which allows anyone to view all of the content and information on their profile. The Facebook can make the content of their page visible only to users that have been confirmed as “Friends,” or visible to both “Friends” and anyone confirmed as a “Friend” of their “Friend” (exponentially increasing the number of people that can view that content). Further, Facebook users can create lists within their “Friends” and allow certain content to be viewed only by subgroups of their Friends (e.g. “Friends” designated as “Work Friends,” or “Family”).

103. The first page of every Facebook account displays a Vanity Name and the space for both a “Profile Picture” and a “Cover Photo.” Facebook users can post additional photos or even entire photo albums. In my training and experience, most Facebook users build their profiles by uploading and changing photographs on their account. Many users own mobile devices that contain cameras, and it is common for mobile cameras and popular camera mobile applications (such as Instagram, an application owned by Facebook) to prompt users to post pictures to their Facebook accounts after a photo is taken.

104. Facebook users have the ability to indicate that other people who appear in their photos are also on Facebook by “tagging” them in the photograph using their Vanity Name. A Facebook user can adjust their privacy settings to require that they confirm a tag before it can be successfully applied.

105. Facebook users can comment on their own photographs and other users’ photographs or indicate that they “Like” a particular image.

106. In addition to photographs, Facebook users can write messages, or “Status Updates,” on their page. This was traditionally referred to as their “wall” or a “wall post,” and is now called a “Timeline.” Unless the user actively deletes them, older postings may be viewable on the users’ account by looking back through the “Timeline.” Facebook users can also add “life events” with a date on their “Timeline,” such as the date they began a particular job or were married. As with photographs and other content, the user can select who can view their posts – allowing them to be visible publicly (the default) or limiting their display to only a selected group of individuals.

107. Facebook users can also send private messages to other Facebook users, as well as to email addresses. These messages are only viewable by the recipient.

108. Facebook users can also create or join “Groups” of other users. Facebook Groups are used by a variety of communities and small groups and are a tool to communicate and share content.

109. Facebook also allows public figures, businesses, organizations, and other entities to create Facebook Pages. Facebook users can become “Fans” of a Facebook Page.

110. Facebook users provide information about their physical location in different ways

through their use of Facebook. Depending on the user's privacy settings, Facebook may also obtain and store the physical location of the user's device(s) as they interact with the Facebook service on those device(s). As described above, Facebook users may also affirmatively state their current address and their hometown. Facebook users may also post Status Updates that discuss where they are, who they are with, and what they are doing. Facebook users who are using a mobile device running the Facebook application may also be able to "Check In" to a location using a feature called "Facebook Places" if the location or establishment from which they are posting offers this feature. The check-in feature allows Facebook users to connect with other users, or "Friends," that are at or near the same location. In addition, Facebook collects other locational information regarding its users, such as the IP address for the device each time the user logs into the site.

111. While it is free to create a profile and use Facebook, Facebook does collect payment information for some uses. Companies that use Facebook can purchase advertisements and sponsored posts. Individual users can use Facebook Marketplace, an online classified service, to sell or purchase items. Facebook users can also purchase games and software applications, and related real or virtual products. Facebook users can also purchase "Facebook Credits" that can then be used for games and application purchases.

112. Facebook encourages connectivity and sharing, and numerous websites now allow users to access services or login to their pages through their Facebook account. In addition, many websites allow users to use Facebook to indicate that the user "Likes" the website, product, or affiliated group. Based on my training, I understand that Facebook also often obtains information regarding other internet activity by its users, even when that user has not actively logged in or

affirmatively selected the “Like” button.

113. Facebook was founded in 2004 and has continually evolved, adding different types of services. In 2012, Facebook announced that it had grown to have more than 1 billion active users.

114. I have viewed the public-facing pages of the Subject Facebook Account. They contain an inset photograph of Augusto and the profile name “Dan Augusto.”

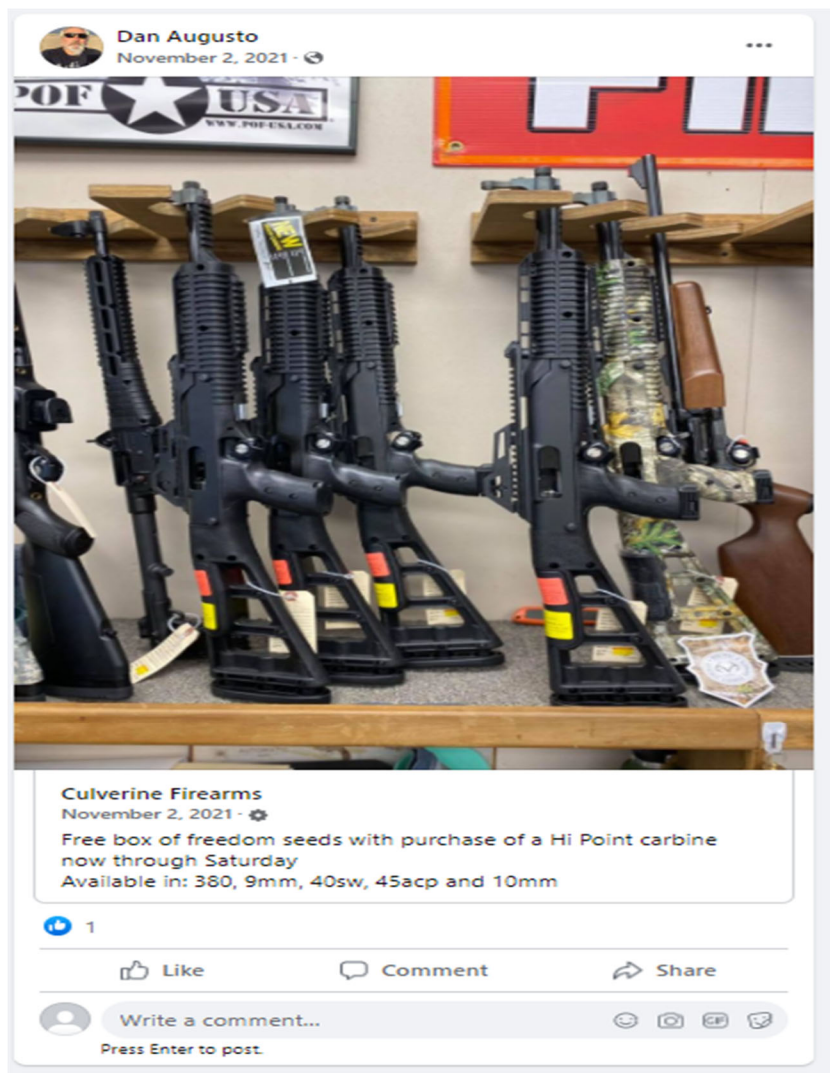
115. On January 31, 2022, Facebook provided information about the Subject Facebook Account pursuant to an Order, dated January 6, 2022, pursuant to 18 U.S.C. § 2703(c) and (d) in Docket No. 22-mj-3002-KAR. According to this information:

- a. The name provided by the account owner is: “Dan Augusto,” which I believe is Augusto.
- b. The account identifier is 100000207447654.
- c. The registered email addresses for the account are: “[daugusto@comcast.net](mailto:daugusto@comcast.net)” (which was listed on the third check to Defense Distributed) and “[dan.augusto.9@facebook.com](mailto:dan.augusto.9@facebook.com)”.
- d. The vanity name with the associated account is: “dan.augusto.9”.
- e. The phone number provided by the account owner is: “+14135373510” (which was listed on the first two checks to Defense Distributed and is listed on Augusto’s Paypal account”).
- f. The PayPal account associated with the Facebook account is: “[pops1002@yahoo.com](mailto:pops1002@yahoo.com)” with a Payment Account ID of “119676172” – *i.e.*, the Paypal account used to purchase the Auto Sear from portablewallhanger.com.


116. Based upon my training, experience, and knowledge of the case, I believe that Augusto owns and operates the Subject Facebook Account.

117. According to my public search of the Subject Facebook Account, Augusto frequently posts photographs of firearms, including the following:


a. November 2, 2021:






b. November 19, 2021:








**Dan Augusto**  
November 19, 2021 · 🌐



**Culverine Firearms**  
November 19, 2021 · ⚙️  
Some Smith Wheels  
686 pro series 7 shot 357mag 5"  
60 pro series 357mag 3"  
610 10mm 4"  
637 38spl... See more

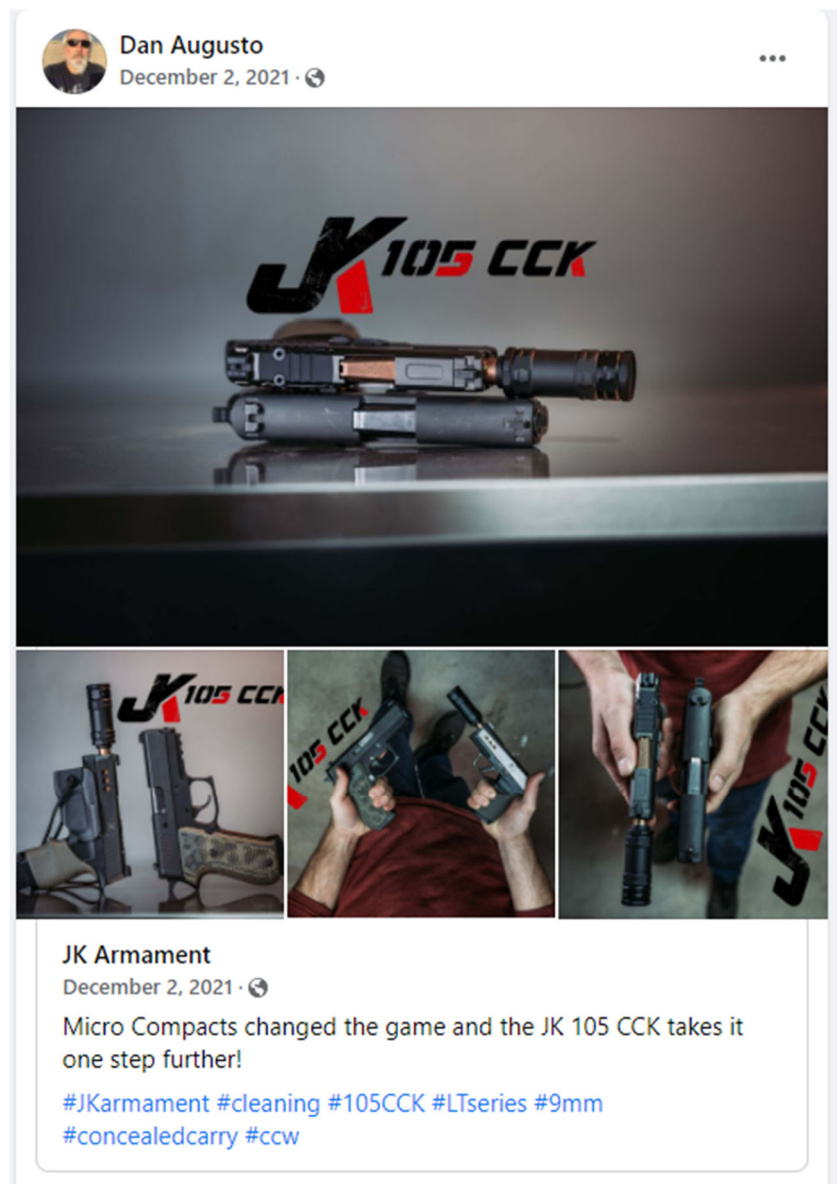
 Like       Comment       Share

 Write a comment...  
Press Enter to post.

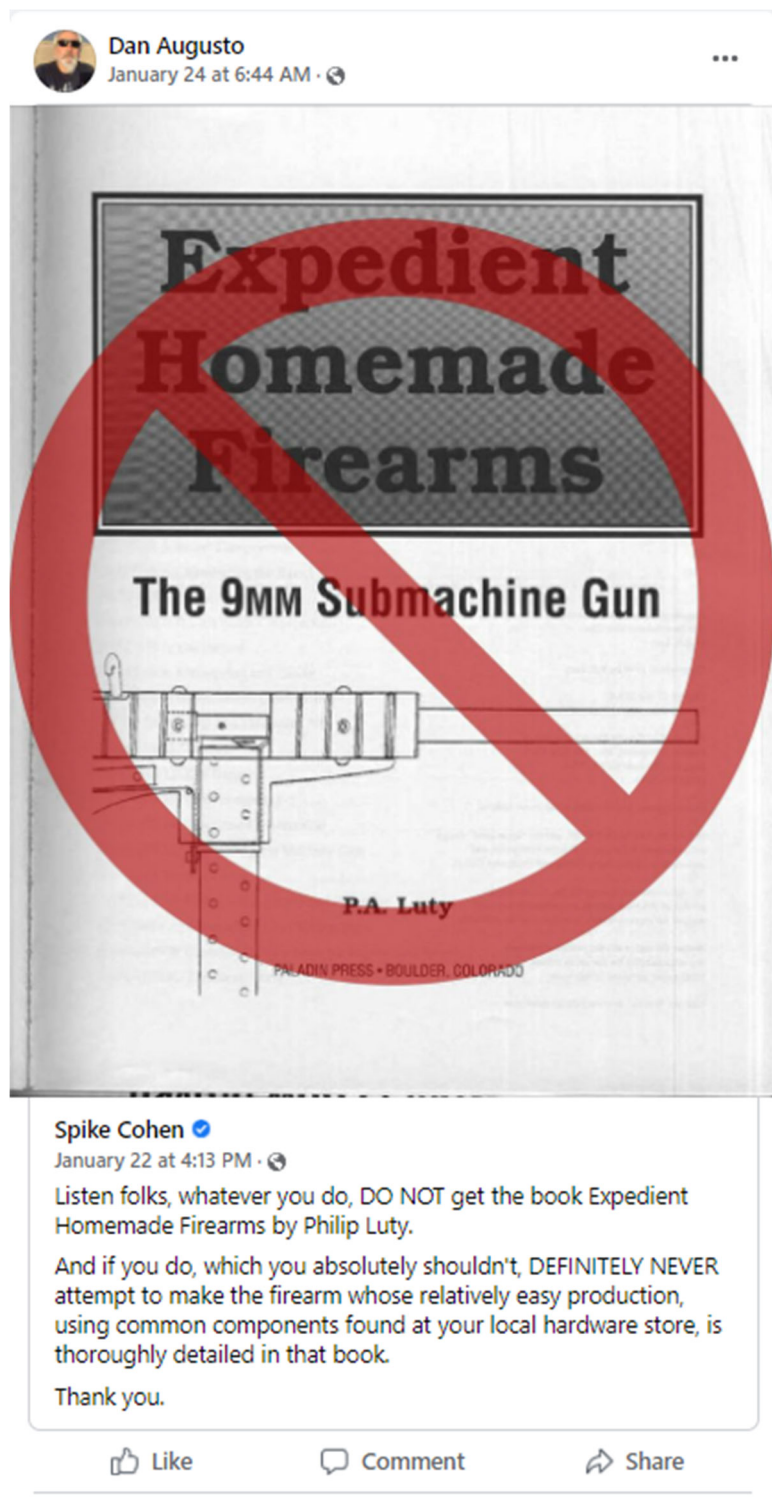
   



c. December 2, 2021:



d. January 22, 2022:



13

118. On February 3, 2022, the ATF submitted a request under 18 U.S.C. § 2703(f) via

the Facebook law enforcement portal that the company preserve all records associated with the Subject Facebook Account. Facebook indicated that it will preserve these records through July 3, 2022.

119. From my training and experience, I am aware that companies that host social-networking accounts, and Facebook in particular, generally maintain records of their subscribers' online activities and private communications unless the user deletes these communications.

The Subject Yahoo Account

120. The Subject Yahoo Account and relevant data is maintained by Oath Holdings, Inc. ("Oath"), which, Government databases indicate, accepts service of process at 701 First Avenue, Sunnyvale, CA 94809 and via its law enforcement portal at [www.yahoo.com](http://www.yahoo.com).

121. On February 16, 2022, the ATF submitted a request under 18 U.S.C. § 2703(f) via the Oath law enforcement portal that the company preserve all records associated with the Subject Yahoo Account. Oath has yet to respond to the preservation request..

122. On January 25, 2022, Oath, through its subsidiary Yahoo, Inc. ("Yahoo") provided information about the Subject Yahoo Account pursuant to an Order, dated January 6, 2022, pursuant to 18 U.S.C. § 2703(c) and (d) in Docket No. 22-mj-3003-KAR. According to this information:

- a. The "other identities" for the account is: "pops1002."
  - b. The "full name" for the account is: "D. Albert Augusto, Sr."
  - c. The "birthdate" for the account is: "1939-10-02."
  - d. The "recovery emails" for the account: "[daugusto@comcast.net](mailto:daugusto@comcast.net) Verified"
- *i.e.*, the same e-mail address listed on the third check to Defense Distributed and

one of the e-mails listed for Augusto's Subject Facebook Account.

e. The "recovery phones" for the account is: "+14135373510" – i.e. the same telephone number listed on the first two checks to Defense Distributed and listed for Augusto's Subject Facebook Account.

123. Based upon my training, experience, and knowledge of the case, including the fact that Augusto's father is now deceased, I believe that Augusto currently owns and operates the Subject Yahoo Account.

124. As set forth above, Augusto has listed the Subject Yahoo Account with his PayPal account, including his PayPal transactions for the Auto Sear purchased on February 9, 2020 and the solvent trap items purchased on December 20 and 24, 2020.

125. According to my review of the "mail header" information for the Subject Yahoo Account provided by Oath, between November 11, 2007, and January 11, 2022, there were approximately 476 e-mail communications between the Subject E-Mail Account and e-mail accounts identified as belonging to PayPal, although none during 2020.

126. In contrast, according to my review of the PayPal account activity logs, between February 24, 2020 and December 31, 2020, there were 297 events logged with the "Actor" being the Subject Yahoo Account.

127. One of these events, with the "Activity" listed as "Auth flow pending" took place on December 20, 2020 at 17:11:50 hours. The "Action Data" for that event reads: "Auth Challenge:EMAIL Metadata: Email sent to : pops1002@yahoo.com..."<sup>14</sup> The time of this event

---

<sup>14</sup> Based upon my training and experience, I believe this indicates that an email was sent on this date from PayPal to the Subject Yahoo Account.

coincides with the date and approximate time of Augusto's \$73.55 purchase of "8.6 inch OD 1.7 Aluminum Car Fuel Filter Solvent Traps cups adapter 5/8x24 & 1/2x28 For NAPA 4003 WIX 24003."

128. Three of these events, listed as "Mobile Login (WAP)," took place on December 24, 2020, at 15:59:23, 15:59:25, and 15:59:28. This date and these times coincide with Augusto's \$99.89 purchase of "Aluminum sprial [sic] 1/2x28 Fuel Filter For NaPa [sic] 4003 Car 8.8 inch solvent traps adapter US."

129. Further, after conducting my review of the "mail header" information for the Subject Yahoo Account, I observed over one thousand e-mail interactions with firearms industry related businesses.<sup>15</sup>

130. E-mail providers such as Oath typically maintain electronic records relating to their customers. These records include account application information, account access information, and e-mail transaction information.

131. Many e-mail providers can also provide the following additional information associated with a subscriber's account: address books; buddy lists; photos, files, data, or other information; and World-Wide Web profiles or homepages.

#### ***SEIZURE OF COMPUTER EQUIPMENT AND DATA***

132. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by

---

<sup>15</sup> The vast majority of these e-mails appear to be automatically generated e-mails of the type that are sent daily to a prospective customer's e-mail address as a type of advertising tool. These e-mails are typically initiated by the customer voluntarily signing up for the advertisements with or without making a purchase from that website.

communicating about them through e-mail, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

133. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

134. I am aware of a report from the United States Census Bureau that shows that in 2016, among all households nationally, 89 percent had a computer, which includes smartphones, and 81 percent had a broadband Internet subscription. Specifically, in 2016, when the use of smartphone ownership was measured separately for the first time, 76 percent of households had a smartphone and 58 percent of households had a tablet, and 77 percent of households had a desktop or laptop computer. Further, according to the Pew Research Center, as of 2019, 96 percent of adult Americans own a cellphone, and 81 percent own a cellphone with significant computing capability (a "smartphone"). The percentage of adults that own a smartphone is even higher among younger demographic groups: 96 percent of 18-29 year olds, 92 percent of 30-49 year olds, and 79 percent of 50-64 year olds owned smartphones in 2019. From my training and experience, I also know

that individuals like Augusto are likely to carry a smartphone with them when they are outside their residence or vehicle.

135. From my training and experience, I am aware that personal computer systems are generally capable of creating, receiving, and otherwise processing computer files generated at or to be used at a business, even an informal business such as personally manufactured firearms, including e-mail, word-processing documents, photographs, and spreadsheets. From my training, experience, and information provided to me by other agents, I am aware that businesses and individuals commonly store records of the type described in Attachment B in computer hardware, computer software, smartphones, and storage media.

136. As set forth above, Augusto has conducted computer-driven, online PayPal purchases of firearms-related items, including the Auto Sear and the solvent trap items as well as used a computer to post firearms-related photographs and other information on the Subject Facebook Account.

137. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after files have been deleted, they can be recovered months or years

later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media — in particular, computers’ internal hard drives — contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage



medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can

indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password

protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

j. In addition, based on my knowledge, training, and experience, I know that businesses and businesspeople often retain correspondence, financial, transactional, and other business records for years to identify past customers and vendors for

potential future transactions; keep track of business deals; monitor payments, debts, and expenses; resolve business disputes stemming from past transactions; prepare tax returns and other tax documents; and engage in other business-related purposes.

138. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media (“computer equipment”) be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

- a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.
- b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to

specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

139. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

140. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner’s knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

141. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution

of the search, reasonably appear to contain the evidence in Attachment B. If however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

142. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any Government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the Government, attorney support staff, and technical experts. Pursuant to this warrant, the agents may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the Government and their support staff for their independent review.

#### ***UNLOCKING A DEVICE USING BIOMETRIC FEATURES***

143. I know from my training and experience, as well as from information found in publicly available materials, that some models of cellphones made by Apple and other manufacturers, offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

144. On the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor.

In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

145. The passcode that would unlock any device(s) found during the search of the Subject Residence is not currently known to law enforcement. Thus, it may be useful to press the finger(s) of the user(s) of any device found during the search of the Subject Residence to the device's fingerprint sensor or to hold the device up to the face of the owner in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. The Government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

146. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises

without any identifying information on the exterior of the device. Thus, it may be necessary for law enforcement to have the ability to require any occupant of the Subject Residence to press their finger(s) against the sensor of the locked device(s) or place the devices in front of their faces in order to attempt to identify the device's user(s) and unlock the device(s).

147. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of Augusto and any individuals found at the Subject Residence to the sensor of the devices or place the devices in front of their faces for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

### **LEGAL AUTHORITY**

148. The Government may obtain both electronic communications and subscriber information by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

149. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the Internet company or e-mail provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

150. If the Government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

151. This application seeks a warrant to search all responsive records and information under the control of Facebook and Oath subject to the jurisdiction of this court, regardless of where the company has chosen to store such information. Pursuant to 18 U.S.C. § 2713, the Government intends to require the disclosure pursuant to the requested warrant of the contents of wire or



electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within the company's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

**REQUEST TO SEAL AND PRECLUDE NOTICE TO THE SUBSCRIBER**

152. I request that this application, the warrant, the order, and any related papers be sealed by the Court until such time as the Court directs otherwise, except that the Government may later produce copies of the search warrant and related documents to the defense during discovery in any criminal case.

153. I further request that, pursuant to the non-disclosure provisions of 18 U.S.C. §§ 2705(b), the Court order Facebook and Oath not to notify any person (including the subscribers or customers to which the materials relate) of the existence of this application, the warrant, the Order, or the execution of the warrant, for a period of one year from the date of this Order, or until notified by the government within thirty days of the conclusion of the investigation, whichever is earlier. Facebook and Oath may disclose this Order to an attorney for Facebook for the purposes of receiving legal advice.

154. Non-disclosure is appropriate in this case because the Court's order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the existence of the investigation. There is accordingly reason to believe that notification of the existence of the Order will seriously jeopardize the investigation, including by giving subjects an opportunity to destroy or tamper with evidence and/or change patterns of behavior. *See* 18 U.S.C. § 2705(b). Moreover, some of the

evidence in this investigation is stored electronically. If alerted to the existence of the Order, the targets could destroy that evidence, including information saved to their personal computers, on other electronic media, or in social media accounts.

#### **FOURTEEN-DAY RULE FOR EXECUTION OF THE WARRANT**

155. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the Government to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the Court issues this warrant, the Government will execute it not by entering the premises of Facebook or Oath, as with a conventional warrant, but rather by serving a copy of the warrant on the companies and awaiting their production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

156. Based on the training and experience of myself and other law enforcement, I understand that e-mail and social media providers sometimes produce data in response to a search warrant outside the 14-day (formerly 10-day) period set forth in Rule 41 for execution of a warrant. I also understand that electronic communication companies sometimes produce data that was created or received after this 14-day deadline ("late-created data"). The Government does not ask for this extra data or participate in its production.

157. Should Facebook or Oath produce late-created data in response to this warrant, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s) absent a follow-up warrant. However, I request permission to view all late-created data that was created by Facebook or Oath, including subscriber, IP address, logging, and other transactional data, without a further order of the Court. This information could

also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit.

158. For these reasons, I request that the Court approve the procedures in the respective Attachments B, which set forth these limitations.

### **CONCLUSION**

159. Based on the information described above, I have probable cause to believe that that Augusto and/or others at the Subject Residence has committed, is committing, and will continue to commit the Subject Offenses.

160. Based on above information uncovered in my investigation and my training and experience, I believe there is probable cause to believe that the Subject Residence, the Subject Facebook Account, the Subject Yahoo Account, and Augusto's person as described in Attachment A-1, A-2, A-3, and A-4 contain the evidence and instrumentalities of violations of the Subject Offenses listed above, as described in Attachment B-1, B-2, B-3, and B-4, including firearms; firearms paraphernalia such as auto-sears, mufflers and silencers; and various records, including financial records, shipping records, shipping labels, tracking numbers, photographs, and contact information of Augusto's associates and potential firearms customers.

161. Therefore, I have probable cause to believe that Augusto has committed violations of the Subject Offenses and that the Subject Residence, the Subject Facebook Account, the Subject Yahoo Account, and Augusto's person contain fruits, evidence, and instrumentalities of these crimes.

I declare that the foregoing is true and correct.

Signed electronically with authorization from  
ATF Special Agent John McKee on February 17, 2022.

/s/ John McKee

JOHN McKEE  
Special Agent, ATF

Subscribed and sworn to before me on February 17, 2022

/s/ Katherine A. Robertson

KATHERINE A. ROBERTSON  
United States Magistrate Judge

Signed electronically with authorization from  
Katherine A. Robertson, U.S. Magistrate Judge on February 17, 2022.



Certified to be a true and  
correct copy of the original  
Robert M. Farrell, Clerk  
U.S. District Court  
District of Massachusetts

By: Melissa H. Rivera  
Deputy Clerk

Date: 02/17/2022

**ATTACHMENT A-1**

**5 Robert Drive, Holyoke, MA**

**PREMISES TO BE SEARCHED**

The premises to be searched are located at 5 Robert Drive, Holyoke, MA, including any outbuildings, sheds, and storage locations. The residence at 5 Robert Drive is a two-floor, single-family home with brown-colored siding, a driveway, and an in-home garage on the north side, a raised porch from the top floor, and in-ground pool on the west side, and a white door with white sidelights on the east side. Photographs of the residence are set forth below:







**ATTACHMENT B-1**

**ITEMS TO BE SEIZED**

1. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 922(a)(6) (False Statements Regarding Sales And Disposition Of Firearms); 922(o) (Unlawful Possession and Transfer of Machinegun), 924(a)(1)(A) (False Statements Regarding Records Of Federal Firearms Licensees), 922(a)(1)(A) (Unlawful Manufacturing and/or Dealing Firearms Without Being Licensed), and 26 U.S.C. §§ 5861(d) and 5845(a)(6)-(7) (Unlawful Receipt And Possession Of Machineguns And Silencers) (the “Subject Offenses”), including:

- a. Records and tangible objects pertaining to the following
  - i. Machineguns or fully-automatic firearms;
  - ii. Auto-sears, conversion kits, and other parts that enable semi-automatic firearms to operate as fully automatic, including so-called hooks and wall hangers;
  - iii. Timothy John Watson and [portablewallhanger.com](http://portablewallhanger.com);
  - iv. Silencers and mufflers, including fuel can and solvent trap equipment;
  - v. Equipment, parts, tools, software, and manuals used to manufacture firearms, including drill presses, milling machines, computer numerical control (“CNC”) milling machines and routers; starter kits; and 80% lowers and frames;
  - vi. The ownership, possession, use, sale, transfer, and disposition of all firearms located inside the Subject Residence, including personally

manufactured firearms, as well as all firearms listed in Exhibit 2.

vii. The existence, identity, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the Subject Offenses.

b. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

i. evidence of who used, owned, or controlled the computer equipment;

ii. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other computer hardware or storage media;

iv. evidence of counter-forensic programs and associated data that are designed to eliminate data;

v. evidence of when the computer equipment was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

vii. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage; and

c. Records and tangible objects relating to the ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check



registers).

2. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph 1. During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of Daniel A. Augusto, Jr. and any individuals found at the Subject Residence to the sensor of the subject device and/or to hold the device in front of their faces.

## **DEFINITIONS**

For the purpose of this warrant:

- A. “Computer equipment” means any computer hardware, computer software, mobile phone, storage media, and data.
- B. “Computer hardware” means any electronic device capable of data processing (such as a computer, smartphone, cell/mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. “Computer software” means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. “Storage media” means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- E. “Data” means all information stored on storage media of any form in any storage format and for any purpose.
- F. “A record” is any communication, representation, information or data. A “record” may be comprised of letters, numbers, pictures, sounds or symbols.

#### **RETURN OF SEIZED COMPUTER EQUIPMENT**

If the owner of the seized computer equipment requests that it be returned, the Government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the Government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy’s authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.

**ATTACHMENT A-2**

**PREMISES TO BE SEARCHED**

**Facebook**

The premises to be searched and seized are (1) the Facebook account associated with identifier number 100000207447654, identifier name dan.augusto.9, and registered e-mail addresses [daugusto@comcast.net](mailto:daugusto@comcast.net) and [dan.augusto.9@facebook.com](mailto:dan.augusto.9@facebook.com); (2) other user-generated data stored with this account; and (3) associated subscriber, transactional, and user connection information associated with the account, as described further in Attachment B. This information is maintained by Facebook, Inc., which accepts service of process at 1601 Willow Road, Menlo Park, CA 94025 and via its law enforcement portal at [www.facebook.com/records](http://www.facebook.com/records).

**ATTACHMENT B-2  
FACEBOOK**

**I. Search Procedure**

A. Within fourteen days of the search warrant's issue, the warrant will be served on Facebook personnel, who will identify the accounts and files to be searched, as described in Section II below.

B. The company will then create an exact electronic duplicate of these accounts and files ("the account duplicate").

C. The company will provide the account duplicate to law enforcement personnel.

D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.

E. Law enforcement personnel may review the account duplicate, even if the company produced it after fourteen days from the warrant's issue, subject to the following limitations. If the company provided data that was created after fourteen days from the warrant's issue ("late-created data"), law enforcement personnel may view all late-created data that was created by the company, including subscriber, IP address, logging, and other transactional data, without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail, absent a follow-up warrant.

**II. Accounts and Files to Be Copied by Company Personnel**

A. All data files associated with the account associated with identifier number 100000207447654, identifier name dan.augusto.9, and registered e-mail addresses [daugusto@comcast.net](mailto:daugusto@comcast.net) and [dan.augusto.9@facebook.com](mailto:dan.augusto.9@facebook.com) (the "Subject Facebook Account") within the possession, custody, or control of the Company, "regardless of whether such

communication, record, or other information is located within or outside of the United States,” *see* 18 U.S.C. § 2713, including any materials preserved on February 3, 2022, when the preservation request was initiated on this account, in the following categories:

1. Biographical profile information entered by the user, including data characterized by Facebook, in the following categories:
  - “About Me”;
  - “Date of Birth”;
  - “Education”;
  - “Favorite Quotes”;
  - “Gender”;
  - “Hometown”;
  - “Physical Tokens” (“Badges” added by the user to the account);
  - “Work”.
2. Information regarding the user’s activities on Facebook and on pages with Facebook connections visited while connected to Facebook, including data characterized by Facebook in the following categories:
  - “Ads Clicked”;
  - “Ad Topics”;
  - “Apps” subscribed to;
  - “Likes on Other Sites”;
  - “Privacy Settings”;
  - “Recent Activities”;
  - “Searches”;
  - Web pages visited that have a Facebook “Like” button;

3. Communications and messages published, sent or received by the user, including data characterized by Facebook in the following categories:
  - “Chat”;
  - “Messages”;
  - “Notes”;
  - “Photos”;
  - “Your Posts”;
  - “Posts By Others”;
  - “Shares”;
  - “Status Updates”;
  - “Videos”
4. Information about the user’s associates, including data characterized by Facebook in the following categories:
  - “Connections”;
  - “Deleted Friends”;
  - “Family”;
  - “Followers”;
  - “Following”;
  - “Friend Requests”;
  - “Friends”;
  - “Groups”;
  - “Hidden from News Feed” (Friends, apps, or pages hidden from news feed);
  - “Likes on Other’s Posts”;
  - “Likes on Your Posts from others”;

- “Networks”;
- “Pending Friend Requests”;
- “Photos”;
- “Pokes”;
- “Removed Friends”;
- “Tag Suggestions Template” (used to help friends “tag” the user in photos that are uploaded)

5. Information regarding the user’s physical location and movements, including all physical location data collected by Facebook’s location services via the user’s mobile phone or other device, and information characterized by Facebook in the following categories:

- “Check-ins”;
- “Current City”;
- “Events”;
- “Last Location”;
- “Locale”;
- “Photos Metadata” (EXIF);

B. All subscriber and transactional records for this account and any associated accounts, including Instagram accounts linked to this account:

1. Names, including;

- “Name”
- “Alternate Name”
- “Name Changes”
- “Screen Names”
- “Vanity URL”

2. Addresses, including;
  - “Address”
  - “Emails” (addresses, including removed addresses)
  - “IP Addresses”
3. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions, including;
  - “Active Sessions”
  - “Logins”
  - “Logouts”
4. Length of service and types of service used, including;
  - “Account Status History”
  - “Registration Date”
  - “Notification Settings”;
  - “Privacy Settings”;
  - List of Types of Facebook services used (*e.g.*, “Messages,” “Notes”)
5. Telephone or instrument numbers, including;
  - “Phone Numbers”
6. Other subscriber numbers or identities, including;
  - “Pages You Admin”
  - “Linked Accounts”
7. Means and source of payment, including;
  - “Credit Cards”
  - “Currency”



### **III. Records and Data to be Searched and Seized by Law Enforcement Personnel**

A. All records and data, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 922(a)(6) (False Statements Regarding Sales And Disposition Of Firearms); 922(o) (Unlawful Possession and Transfer of Machinegun), 924(a)(1)(A) (False Statements Regarding Records Of Federal Firearms Licensees), 922(a)(1)(A) (Unlawful Manufacturing and/or Dealing Firearms Without Being Licensed), and 26 U.S.C. §§ 5861(d) and 5845(a)(6)-(7) (Unlawful Receipt And Possession Of Machineguns And Silencers) (the “Subject Offenses”), including records or data relating to:

1. Machineguns or fully-automatic firearms;
2. Auto-sears, conversion kits, and other parts that enable semi-automatic firearms to operate as fully automatic, including so-called hooks and wall hangers;
3. Timothy John Watson and [portablewallhanger.com](http://portablewallhanger.com);
4. Silencers and mufflers, including fuel can and solvent trap equipment;
5. Equipment, parts, tools, software, and manuals used to manufacture firearms, including drill presses, milling machines, computer numerical control (“CNC”) milling machines and routers; starter kits; and 80% lowers and frames;
6. The ownership, possession, use, sale, transfer, and disposition of all firearms located inside 5 Robert Drive, Holyoke, MA, including personally manufactured firearms, as well as all firearms listed in Exhibit 2.
7. Computer activity in furtherance of activities related to the Subject Offenses;

8. The identity and past or present location of the user(s) of the Subject Facebook Account and any co-conspirators;
  9. The identity, location, and ownership of any computers used to access the Subject Facebook Account;
  10. Other e-mail or Internet accounts, telephone numbers, social media services, or web or mobile based applications providing Internet access, remote data storage, or communication services for Daniel A. Augusto, Jr., and any co-conspirators;
  11. The sources of income, and the location of, and identifiers for, bank accounts, e-currency accounts, and credit accounts for Daniel A. Augusto and any co-conspirators; and
- B. All of the subscriber, transactional, and logging records described in Section II (B).

**ATTACHMENT A-3**

**PREMISES TO BE SEARCHED**

**Oath Holdings, Inc. / Yahoo, Inc.**

The premises to be searched and seized are (1) the e-mail account identified as [pops1002@yahoo.com](mailto:pops1002@yahoo.com); (2) other user-generated data stored with this account; and (3) associated subscriber, transactional, and user connection information associated with the account, as described further in Attachment B. This information is maintained by Oath Holdings, Inc., which accepts service of process at 701 First Avenue, Sunnyvale, CA 94809 and via its law enforcement portal at [www.yahoo.com](http://www.yahoo.com).

**ATTACHMENT B-3**  
**Oath Holdings, Inc. / Yahoo, Inc.**

**I. Search Procedure**

A. Within fourteen days of the search warrant’s issue, the warrant will be served on Oath/Yahoo personnel, who will identify the accounts and files to be searched, as described in Section II below.

B. The company will then create an exact electronic duplicate of these accounts and files (“the account duplicate”).

C. The company will provide the account duplicate to law enforcement personnel.

D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.

E. Law enforcement personnel may review the account duplicate, even if the company produced it after fourteen days from the warrant’s issue, subject to the following limitations. If the company provided data that was created after fourteen days from the warrant’s issue (“late-created data”), law enforcement personnel may view all late-created data that was created by the company, including subscriber, IP address, logging, and other transactional data, without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail, absent a follow-up warrant.

**II. Accounts and Files to Be Copied by Company Personnel**

A. All data files associated with the e-mail account associated with [pops1002@yahoo.com](mailto:pops1002@yahoo.com) (the “Subject Yahoo Account”) within the possession, custody, or control of the Company, “regardless of whether such communication, record, or other information is located within or outside of the United States,” *see* 18 U.S.C. § 2713, including any materials

preserved on or about February 16, 2022, when the preservation request was initiated on this account, in the following categories:

1. The contents of all e-mail, whether draft, deleted, sent, or received;
  2. The contents of all text or instant messages;
  3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;
  4. The contents of all calendar data;
  5. Lists of friends, buddies, contacts, or other subscribers;
  6. Records pertaining to communications between the company and any person regarding these accounts and any e-mail accounts associated with those addresses, including contacts with support services and records of actions taken.
- B. All subscriber and transactional records for the Subject Yahoo Account and any associated e-mail accounts, including:
1. Subscriber information for these and any associated e-mail accounts:
    - a. Name(s) and account identifiers;
    - b. Address(es);
    - c. Records of session times and durations;
    - d. Length of service (including start date) and types of service utilized;
    - e. Telephone instrument number or other subscriber number or identity, including any temporary assigned network address;
    - f. The means and source of payment for such service (including any credit card or bank account number); and
    - g. The Internet Protocol address used by the subscriber to register the

account or otherwise initiate service.

2. User connection logs for any connections to or from these and any associated e-mail accounts, including:
  - a. Connection time and date;
  - b. Disconnect time and date;
  - c. The IP address that was used when the user connected to the service;
  - d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and
  - e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

### **III. Records and Data to be Searched and Seized by Law Enforcement Personnel**

A. All records and data, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 922(a)(6) (False Statements Regarding Sales And Disposition Of Firearms); 922(o) (Unlawful Possession and Transfer of Machinegun), 924(a)(1)(A) (False Statements Regarding Records Of Federal Firearms Licensees), 922(a)(1)(A) (Unlawful Manufacturing and/or Dealing Firearms Without Being Licensed), and 26 U.S.C. §§ 5861(d) and 5845(a)(6)-(7) (Unlawful Receipt And Possession Of Machineguns And Silencers) (the “Subject Offenses”), including records or data relating to:

1. Machineguns or fully-automatic firearms;
2. Auto-sears, conversion kits, and other parts that enable semi-automatic firearms to operate as fully automatic, including so-called hooks and wall hangers;
3. Timothy John Watson and [portablewallhanger.com](http://portablewallhanger.com);

4. Silencers and mufflers, including fuel can and solvent trap equipment;
  5. Equipment, parts, tools, software, and manuals used to manufacture firearms, including drill presses, milling machines, computer numerical control (“CNC”) milling machines and routers; starter kits; and 80% lowers and frames;
  6. The ownership, possession, use, sale, transfer, and disposition of all firearms located inside 5 Robert Drive, Holyoke, MA, including personally manufactured firearms, as well as all firearms listed in Exhibit 2.
  7. Computer activity in furtherance of activities related to the Subject Offense;
  8. The identity and past or present location of the user(s) of the Subject Facebook Account and any co-conspirators;
  9. The identity, location, and ownership of any computers used to access the Subject Facebook Account;
  10. Other e-mail or Internet accounts, telephone numbers, social media services, or web or mobile based applications providing Internet access, remote data storage, or communication services for Daniel A. Augusto, Jr., and any co-conspirators;
  11. The sources of income, and the location of, and identifiers for, bank accounts, e-currency accounts, and credit accounts for Daniel A. Augusto and any co-conspirators; and
- B. All of the subscriber, transactional, and logging records describe in Section II(B).

**ATTACHMENT A-4**

**PREMISES TO BE SEARCHED**

**The Person of Daniel A. Augusto, Jr.**

The premises to be searched and seized are the person of Daniel A. Augusto, Jr.



**ATTACHMENT B-4**

**The Person of Daniel A. Augusto, Jr.**

**ITEMS TO BE SEIZED**

1. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 922(a)(6) (False Statements Regarding Sales And Disposition Of Firearms); 922(o) (Unlawful Possession and Transfer of Machinegun), 924(a)(1)(A) (False Statements Regarding Records Of Federal Firearms Licensees), 922(a)(1)(A) (Unlawful Manufacturing and/or Dealing Firearms Without Being Licensed), and 26 U.S.C. §§ 5861(d) and 5845(a)(6)-(7) (Unlawful Receipt And Possession Of Machineguns And Silencers) (the “Subject Offenses”), including:

- a. Records and tangible objects pertaining to the following
  - i. Machineguns or fully-automatic firearms;
  - ii. Auto-sears, conversion kits, and other parts that enable semi-automatic firearms to operate as fully automatic, including so-called hooks and wall hangers;
  - iii. Timothy John Watson and [portablewallhanger.com](http://portablewallhanger.com);
  - iv. Silencers and mufflers, including fuel can and solvent trap equipment;
  - v. Equipment, parts, tools, software, and manuals used to manufacture firearms, including drill presses, milling machines, computer numerical control (“CNC”) milling machines and routers; starter kits; and 80% lowers and frames;
  - vi. The ownership, possession, use, sale, transfer, and disposition of all

firearms located inside 5 Robert Drive, Holyoke, MA, including personally manufactured firearms, as well as all firearms listed in Exhibit 2.

vii. The existence, identity, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the Subject Offenses.

b. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

- i. evidence of who used, owned, or controlled the computer equipment;
- ii. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;
- iii. evidence of the attachment of other computer hardware or storage media;
- iv. evidence of counter-forensic programs and associated data that are designed to eliminate data;
- v. evidence of when the computer equipment was used;
- vi. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
- vii. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage; and

2. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph 1. During the

execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of Daniel A. Augusto, Jr. and any individuals found at the Subject Residence to the sensor of the subject device and/or to hold the device in front of their faces.

## DEFINITIONS

For the purpose of this warrant:

- G. “Computer equipment” means any computer hardware, computer software, mobile phone, storage media, and data.
- H. “Computer hardware” means any electronic device capable of data processing (such as a computer, smartphone, cell/mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- I. “Computer software” means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- J. “Storage media” means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- K. “Data” means all information stored on storage media of any form in any

storage format and for any purpose.

- L. “A record” is any communication, representation, information or data. A “record” may be comprised of letters, numbers, pictures, sounds or symbols.

#### **RETURN OF SEIZED COMPUTER EQUIPMENT**

If the owner of the seized computer equipment requests that it be returned, the Government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the Government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy’s authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.